QUALIFICACIÓ

2.5

Assignatura:

Estudiant/a: [redacted]

Data:

Problema 1.

$$A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

$p \in \mathbb{Z}$ nombre primer senar $(p \neq 2)$.

$a \in \mathbb{Z}$ tq $a^2 \equiv 2 \pmod p$.

(a) Exemple:

$p = 7$ $\quad a = 3 \Rightarrow a^2 = 9 = 2 \pmod 7$

0.25 ✓ $\quad a = 4 \Rightarrow a^2 = 16 = 2 \pmod 7$

(b) Anem a fer servir el fet que $a^2 \equiv 2 \pmod p$.

$$\varphi_1 : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}/p\mathbb{Z} \qquad (\text{idea naïf: } \sqrt{2} \simeq \pm a)$$

$$x + y\sqrt{2} \longmapsto \overline{x + ya}$$

~~Error.~~

$$\varphi_2 : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

on $\overline{k}$ simbolitza $\boxed{\overline{k} = k \pmod p}$

$$x + y\sqrt{2} \longmapsto \overline{x - ya}$$

✓

1r. Estan ben definits? $\varphi_{\frac{1}{2}}(z) \in \mathbb{Z}/p\mathbb{Z}$??

Donat $z \in \mathbb{Z}[\sqrt{2}] \Rightarrow z = x + \sqrt{2}y$, $x, y \in \mathbb{Z}$

(identificació única)

$\varphi_1(z) = \overline{x + ay}$, amb $x \pm ay \in \mathbb{Z}$

$\varphi_2(z) = \overline{x - ay} \Rightarrow \varphi_1(z), \varphi_2(z) \in \mathbb{Z}/p\mathbb{Z}$ ✓

2n Són morfismes? ✓

- $\varphi_1(1) = \overline{1 + a0} = \overline{1} = 1 \pmod p$ ✓
- $\varphi_2(1) = \overline{1 - a0} = \overline{1} = 1 \pmod p$ ✓
- $\varphi_{\frac{1}{2}}\left((x_1 + \sqrt{2}y_1) + (x_2 + \sqrt{2}y_2)\right)$ (Ho fem a la vegeda pq només canvia un signe!!)

$= \varphi_{\frac{1}{2}}\left((x_1 + x_2) + (y_1 + y_2)\sqrt{2}\right) = \overline{x_1 + x_2 \pm a y_1 \pm y_2 a}$

$= \overline{x_1 \pm a y_1} + \overline{x_2 \pm a y_2} = \varphi_{\frac{1}{2}}(x_1 + y_1\sqrt{2}) + \varphi_{\frac{1}{2}}(x_2 + y_2\sqrt{2})$ ✓

- $\varphi_{\frac{1}{2}}\left((x_1 + y_1\sqrt{2}) \cdot (x_2 + y_2\sqrt{2})\right) =$

$= \varphi_{\frac{1}{2}}\left((x_1x_2 + 2y_1y_2) + (y_1x_2 + x_1y_2)\sqrt{2}\right) =$

$\overline{x_1x_2 + 2y_1y_2 \pm a(y_1x_2 + x_1y_2)} =$

$= \bar{x}_1\bar{x}_2 + \bar{a}^2\bar{y}_1\bar{y}_2 \pm \bar{a}\bar{y}_1\bar{x}_2 \pm \bar{a}\bar{y}_2\bar{x}_1$

$\bar{a}^2 = \bar{2}$ $= (\bar{x}_1 \pm a\bar{y}_1)(\bar{x}_2 \pm a\bar{y}_2)$

$= \varphi_{\frac{1}{2}}(x_1 + y_1\sqrt{2})\,\varphi_{\frac{1}{2}}(x_2 + y_2\sqrt{2})$ ✓

on $\varphi_{\frac{1}{2}}$ val $\begin{cases} + \to \varphi_1 \\ - \to \varphi_2 \end{cases}$.

Per tant, φ_1, φ_2 morfismes. ✓ 1

(c) Siguin els $\mathrm{Nuc}(\varphi_1)$, $\mathrm{Nuc}(\varphi_2) \subseteq A$.

Pel primer teorema de isomorfisme.

$$\frac{A}{\mathrm{Nuc}(\varphi_1)} \cong \mathrm{Im}(\varphi_1) \qquad \frac{A}{\mathrm{Nuc}(\varphi_2)} \cong \mathrm{Im}(\varphi_2)$$

A més, podem veure que φ_1 i φ_2 són exhaustives.

$\forall\, \bar{b} \in \mathbb{Z}/p\mathbb{Z} \Rightarrow \bar{b} \equiv b \pmod p$ ✓

Llavors.

$\varphi_1(b + 0\sqrt{2}) = \overline{b + 0\cdot a} = \bar{b}$ ✓

$\varphi_2(b + 0\sqrt{2}) = \overline{b - 0\cdot a} = \bar{b}$ ✓

on $b \in \mathbb{Z}$.

Per tant, $\forall \bar{b} \in \mathbb{Z}/p\mathbb{Z}$, $\bar{b} \in Im(\varphi_1), Im(\varphi_2)$.

$\Rightarrow Im(\varphi_1) = \mathbb{Z}/p\mathbb{Z} = Im(\varphi_2)$.

Per tant,

$$\frac{A}{Nuc(\varphi_1)} \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \qquad \frac{A}{Nuc(\varphi_2)} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$$

Com $\mathbb{Z}/p\mathbb{Z}$ és un cos $\Rightarrow$ $Nuc(\varphi_1), Nuc(\varphi_2)$ són maximals. ✓

0.7 ✓

(d) És fals. Tenim un contraexemple amb $Nuc(\varphi_1)$ i $Nuc(\varphi_2)$.

$$\left[\frac{A}{Nuc(\varphi_1)} \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \cong \frac{A}{Nuc(\varphi_2)}\right]$$ vist abans.

Anem a buscar l'aparença de $Nuc(\varphi_1)$.

$$\varphi_1(x+y\sqrt{2}) = 0 \iff \overline{x+ya} = \bar{0} \pmod{p}$$

$$\iff x + ya = pk \qquad k \in \mathbb{Z}$$

$$\iff x = -ya + pk$$

Per tant, $\mathrm{Nuc}(\varphi_1) = \{(-ya+pk) + y\sqrt{2} : y \in \mathbb{Z}, k \in \mathbb{Z}\}$

En canvi, en $\mathrm{Nuc}(\varphi_2)$

$$\varphi_2(x+y\sqrt{2}) = 0 \iff \overline{x+(-y)a} = \bar{0} \pmod p$$

$$\iff x - ya = pn \qquad n \in \mathbb{Z}$$

$$\iff x = ya + pn$$

Per tant, $\mathrm{Nuc}(\varphi_2) = \{(ya+pn) + y\sqrt{2} : y \in \mathbb{Z}, n \in \mathbb{Z}\}$

Anem a veure que

$z = -a + \sqrt{2} \in \mathrm{Nuc}(\varphi_1)$ $(k=0, y=1)$

no pertany a $\mathrm{Nuc}(\varphi_2)$:

Si $z \in \mathrm{Nuc}(\varphi_2) \Rightarrow -a+\sqrt{2} = ya + pn + y\sqrt{2}$

$$\iff y = 1 \quad -a+\sqrt{2} = a + pn + \sqrt{2}$$

$$\iff \boxed{2a = -pn} \qquad n \in \mathbb{Z} \qquad 2 = 0 \pmod p$$

$$\iff \overline{2a} = 0 \pmod p \iff 2a^2 = 0 \pmod p$$

$\Leftarrow$ $\boxed{p=2}$!! ~~Que bé~~ $\Rightarrow \in$

p primer sense !! ✓

$\Rightarrow -a+\sqrt{2} \notin Nuc(\varphi_2)$

$\Rightarrow Nuc(\varphi_1) \neq Nuc(\varphi_2)$ ✓ ✓ 0.5

(e) 1r Fixem-nos que $\mathbb{Z}/p\mathbb{Z}$ és un cos.

$\Rightarrow \mathbb{Z}/p\mathbb{Z}[x]$ és euclidià $\Rightarrow \mathbb{Z}/p\mathbb{Z}[x]$ és DIP

Llavors

$\Rightarrow x^2-2$ irreductible $\Rightarrow (x^2-2)$ maximal.

$\Rightarrow \dfrac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)}$ és un cos.

$= \{ a_0 + a_1\gamma : a_0, a_1 \in \mathbb{Z}/p\mathbb{Z} \}$

i $\gamma^2 - 2 = 0 \pmod p$

2n Si tinguessim un morfisme de A en $\mathbb{Z}/p\mathbb{Z}$,

llavors $A = \dfrac{\mathbb{Z}[x]}{(x^2-2)} \xrightarrow[\text{morf.}]{\varphi} \mathbb{Z}/p\mathbb{Z}$

per def.

QUALIFICACIÓ

Assignatura:

Estudiant/a: [redacted]

Data:

3r llavors utilitzant morfisme d'injecció.

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}$$

$$\Downarrow$$

$$\mathbb{Z}/p\mathbb{Z}[x] \xhookrightarrow{i} \mathbb{Z}[x]$$

$$\Downarrow$$

$$\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)} \xhookrightarrow{i} \frac{\mathbb{Z}[x]}{(x^2-2)}$$

$$\bar{a}_0 + \bar{a}_1 x \longmapsto a_0 + a_1 x \quad !!$$

Tenim un morfisme de $f = \varphi \circ i$

$$\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)} \xhookrightarrow{i} \frac{\mathbb{Z}[x]}{(x^2-2)} \xrightarrow{\varphi} \mathbb{Z}/p\mathbb{Z}$$

$$\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)} \xrightarrow{f} \mathbb{Z}/p\mathbb{Z}$$

És morfisme perquè és composició de morfismes.

A més és injectiu !! perquè $\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)}$ és un cos.

$$\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)} \hookrightarrow \mathbb{Z}/p\mathbb{Z} \quad !!$$

Fixem-nos que per altra banda

$$\mathbb{Z}/p\mathbb{Z} \subset \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)}$$

amb l'injecció canònica $\bar{a} \longmapsto \bar{a} + \bar{0}x$.

Per tant,

$$\mathbb{Z}/p\mathbb{Z} \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)}$$

No obstant això és impossible perquè

$$|\mathbb{Z}/p\mathbb{Z}| = p \quad \# \quad \Rightarrow \Leftarrow$$

$$\left|\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x^2-2)}\right| = p^2 \rightsquigarrow \left(p \cdot p \right\} a_0 + a_1 x : a_0, a_1 \in \mathbb{Z}/p$$

Per tant no existeix $\varphi: \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}/p\mathbb{Z}$ morfisme ▨

Problema 2. K cos, $A = \{ f(x) \in K[x] \mid f'(0) = 0 \}$

(a) A subanell de $K[x]$?

1r. Fixem-nos que $A \subset K[x]$ per definició ✓

2n. • $f(x) = 1 \quad f'(x) = 0 \quad f'(0) = 0$ ✓

$\Rightarrow 1 \in A$ ✓

• Suposem $f, g \in A \Rightarrow f'(0) = 0 \quad g'(0) = 0$

+ $(f+g)'(0) = f'(0) + g'(0) = 0 \Rightarrow f+g \in A$ ✓

+ $(fg)'(0) = \underbrace{f'(0)}_{0} g(0) + f(0) \underbrace{g'(0)}_{0} = 0 \Rightarrow fg \in A$ ✓

↑ Regla Leibniz

+ $(-f)'(0) = -f'(0) = 0 \Rightarrow -f \in A$ ✓

Per tant, A subanell de $K[x]$.

Com $A \subset K[x] \Rightarrow [A^* \subset K[x]^* = K^*]$

les unitats no són K^* són $K^* = K - \{0\}$

Anem a demostrar que $K^* \subset A^*$.

Donat $a \in K$, $(a')(0) = 0 \Rightarrow a \in A$

$\exists\, a^{-1} \in K$; $(a^{-1})'(0) = 0 \Rightarrow a^{-1} \in A$.

$a \cdot a^{-1} = 1 \Rightarrow a \in A^*$ ✓

Per tant, $\boxed{A^* = K^*}$ (vist K com inclòs en $K[x]$)

(b) $f(x) = x^3$ element irreductible en A?

1r. $f \in A$? $f'(x) = 3x^2$ $f'(0) = 0$ ✓

$x^3 \in A$.

2n. és irreductible?

i suposem que no són units

Suposem $x^3 = f(x)\,g(x)$ on $f(x), g(x) \in A \subseteq K[x]$

~~Com $K[x]$ és euclidià, $K[x]$ és factorial i~~

~~x^3 descompon de manera única com a producte de irreductibles.~~ $x^3 = x \cdot x \cdot x$

~~Clarament, sabem que $f(x)$, $g(x)$~~

Com $K[x]$ és euclidia, $K[x]$ és factorial.

x^3 descompon de manera única com a producte de irreductibles de $K[x]$ (x primer pq $\frac{K[x]}{(x)}$ és K integre)

$$f(x)\cdot g(x) = x^3 = x\cdot x\cdot x.$$

Si $f(x), g(x)$ no són unitats,

llavors $\begin{cases} f(x) = x^2 \\ g(x) = x \end{cases}$ o al revés. (sense pèrdua de generalitat)

Llavors tenim que $g(x) = x \Rightarrow$

$$g'(x) = 1 \Rightarrow g'(0) = 1 \neq 0 \Rightarrow g \notin A!!$$ ✓

Per tant, $g(x)$ o $f(x) \in A^*$. 0.5

$\Rightarrow x^3$ és irreductible en A.

(c) Anem primer a demostrar que x^2 també és irreductible en A.

1r. $(x^2)' = 2x \Rightarrow (x^2)'_{x=0} = 2\cdot 0 = 0 \Rightarrow x^2 \in A$ ✓

2n. Suposem $x^2 = f(x)g(x)$, $f(x), g(x) \in A \setminus A^*$

Mirant $x^2 \in K[x]$, sabem que $x^2 = x \cdot x$ de manera única $\Rightarrow$ $\begin{cases} f(x) = x \\ g(x) = x \end{cases}$

Però abans hem vist que $x \notin A$!!

$\Rightarrow$ $f(x)$ o $g(x) \in A^*$. ✓

Sabem que x^2 i x^3 són irreductibles.

Fixem-nos que $((x^6)' = 6x^5 \quad (x^6)'(0) = 0 \Rightarrow x^6 \in A)$

$A \ni x^6 = x^3 \cdot x^3 = x^2 x^2 \cdot x^2$

Té dos descomposicions en elements irreductibles no associats.

$\Rightarrow$ A no és factorial !! ✓ 1/

(d) ideal d'A no principal ??

A no és factorial $\Rightarrow$ A no és DIP $\Rightarrow$ hi ha ideals no principals.

Anem a buscar un.

$I = (x^2, x^3)$ és un bon candidat.

QUALIFICACIÓ

Assignatura: [redacted]

Estudiant/a:

Data:

Suposem que és principal, és a dir,

$$(x^2, x^3) = (m(x)) \quad \text{on } m(x) \in A.$$

Per tant, tindriem que per algun $p(x), q(x) \in A$

$$m(x)\,p(x) = x^2$$

$$m(x)\,q(x) = x^3.$$

Com x^2 i x^3 son irreductibles. (dem abans)

$$\Rightarrow \begin{cases} m(x) = a \\ m(x) = x^2 \cdot b \end{cases} \qquad \begin{cases} m(x) = a \\ m(x) = x^3 \cdot c \end{cases}$$

Per tant, $m(x)$ ha de ser de K.

$$m(x) = a \in K \Rightarrow (m(x)) = (1).$$

$$\Rightarrow (x^2, x^3) = (1).$$

Això, implicaria per Bezout que $\exists\, p(x), q(x) \in A : \in K$

$$p(x)x^2 + q(x)x^3 = 1 = x^2\left(p(x) + q(x)x^3\right) !!$$

Però sabem que $x^2 \notin A^*$!! $\Rightarrow (x^2, x^3)$ no és principal.

(e) Com tot anell euclidià, és principal.
i A no es principal, llavors,
doncs A no és euclidià.
(problema 4)

✓ 0'5

Problema 3. $K = \mathbb{Q}(\sqrt[3]{5})$ $L = \mathbb{Q}(\sqrt[5]{3})$

(a) $M = KL = \mathbb{Q}(\sqrt[3]{5}, \sqrt[5]{3})$

Fixem-nos primer que

- $\alpha = \sqrt[3]{5} \Rightarrow \alpha^3 = 5 \Rightarrow \alpha^3 - 5 = 0$

és un polinom 5-eisenstein $\Rightarrow$ irreductible

Per tant, $[K : \mathbb{Q}] = 3$

- $\beta = \sqrt[5]{3} \Rightarrow \beta^5 = 3 \Rightarrow \beta^5 - 3 = 0$.

és un polinom 3-eisenstein $\Rightarrow$ irreductible

Per tant, $[L : \mathbb{Q}] = 5$.

$\therefore M = \mathbb{Q}(\sqrt[3]{5}, \sqrt[5]{3})$ · $[M : K] \leq 5$

≤ 5 ≤ 3

$K = \mathbb{Q}(\sqrt[3]{5})$ $L = \mathbb{Q}(\sqrt[5]{3})$ perquè $\beta^5 - 3 = 0$ ✓ $x^5 - 3 \in \mathbb{Q}(\sqrt[3]{5})[x]$

3 5

$\mathbb{Q}$

• $[M:L] \leq 3$ pq. $x^3 - 5 \in \mathbb{Q}(\sqrt[5]{3})[x]$

$a^3 - 5 = 0$ ✓

Clarcs també • $[M:\mathbb{Q}] = [M:L] \cdot [L:\mathbb{Q}]$

$= [M:L] \cdot 5$

• $[M:\mathbb{Q}] = [M:K] \cdot [K:\mathbb{Q}] = [M:K] \cdot 3$

• $[M:\mathbb{Q}] \leq 15$. $[M:\mathbb{Q}] \geq 1$.

La única solució entera que ho compleix

és $[M:\mathbb{Q}] = 15 = 3 \cdot 5$

$[M:L] = 3$

$[M:K] = 5$

(b) Una $\mathbb{Q}$-base de K és $\mathbb{Q}\{1, \sqrt[3]{5}, \sqrt[3]{5^2}\}$

Una $\mathbb{Q}$-base de L és $\mathbb{Q}\{1, \sqrt[5]{3}, \sqrt[5]{3^2}, \sqrt[5]{3^3}, \sqrt[5]{3^4}\}$

Un candidata base de L és, si anomenem

$(\alpha = \sqrt[3]{5}, \beta = \sqrt[5]{3})$

$(K = \mathbb{Q}\langle 1, \alpha, \alpha^2 \rangle \quad L = \mathbb{Q}\langle 1, \beta, \beta^2, \beta^3, \beta^4 \rangle)$

QUALIFICACIÓ

Assignatura: [redacted]

Estudiant/a:

Data:

Una candidata és:

$$\{1, \beta, \beta^2, \beta^3, \beta^4, \alpha, \alpha\beta, \alpha\beta^2, \alpha\beta^3, \alpha\beta^4, \alpha^2, \alpha^2\beta, \alpha^2\beta^2, \alpha^2\beta^3, \alpha^2\beta^4\}$$

Anem a demostrar que es base:

- Són l.i?

$\lambda_{ij} \in \mathbb{Q}$

Suposem que tenim $\sum_{j=0}^{4}\sum_{i=0}^{2} \lambda_{ij}\alpha^i\beta^j = 0$

Agrupant les β^j tenim $\sum_{j=0}^{4}\left(\sum_{i=0}^{2}\lambda_{ij}\alpha^i\right)\beta^j = 0$ (*)

Com $[M:K] = 5$ sabem que $gr\left(Irr(\beta, \mathbb{Q}(\alpha), x)\right) = 5$.

Això implica que $\sum_{i=0}^{2}\lambda_{ij}\alpha^i = 0 \quad \forall i$

(*)

(sino el gr ≤ 5). Com α^i són independents en $\mathbb{Q}$

$\Rightarrow$ $\boxed{\lambda_{ij} = 0 \quad \forall i, \forall j}$

Per tant, són l.i. i són 15 elements

$\Downarrow$ $(\dim_{\mathbb{Q}} M = 15)$

generen $M \Rightarrow$ són base ✓

(c)

Atenció!! Canvio l'enunciat a γ enlloc de α pq $\boxed{\alpha = \sqrt[3]{5}}$ $\boxed{\gamma \in L}$!!

Com $\gamma \in L \Rightarrow \left[\gamma = c_0 + c_1\beta + c_2\beta^2 + c_3\beta^3 + c_4\beta^4\right]$

Anem a calcular R_α.

$\gamma \cdot 1 = c_0 + c_1\beta + c_2\beta^2 + c_3\beta^3 + c_4\beta^4$

$\gamma \cdot \beta = \frac{c_4\beta^5}{3c_4} + c_0\beta + c_1\beta^2 + c_2\beta^3 + c_3\beta^4$

$\vdots$

$\gamma^4\beta = 3c_1 + 3c_2\beta + 3c_3\beta^2 + 3c_4\beta^3 + c_0\beta^4$

$\boxed{\beta^5 = 3,\ \beta^6 = 3\beta,\ \beta^7 = 3\beta^2,\ \beta^8 = 3\beta^3}$

QUALIFICACIÓ

Assignatura: [redacted]

Estudiant/a:

Data:

Fixem-nos que l'únic que fora multiplicar per α es que tots els termes tinguin un α (*)

Llavors amb la representació de γ en la base $\{1, \beta, \beta^2, \beta^3, \beta^4\}$ ja fem.

$$M_\gamma = \text{en } \mathbb{Q}(\beta) \begin{pmatrix} c_0 & 3c_4 & 3c_3 & 3c_2 & 3c_1 \\ c_1 & c_0 & 3c_4 & 3c_3 & 3c_2 \\ c_2 & c_1 & c_0 & 3c_4 & 3c_3 \\ c_3 & c_2 & c_1 & c_0 & 3c_4 \\ c_4 & c_3 & c_2 & c_1 & c_0 \end{pmatrix}$$

Llavors aplicant que multiplica per α només fa que canviem a la base $\{\alpha, \beta\alpha, \ldots \beta^4\alpha\}$

Llavors

$$R_\gamma = \left(\begin{array}{c|cc} M_\gamma & 0 & 0 \\ \hline 0 & M_\gamma & 0 \\ 0 & 0 & M_\gamma \end{array}\right)$$

Finalment, el polinomi característic és.

$$P_c(x) = \det(R_a - x\,Id_{15})$$

$$= \det\begin{pmatrix} M_\gamma - x\,Id_5 & C & C \\ C & M_\gamma - x\,Id_5 & C \\ C & C & M_\gamma - x\,Id_5 \end{pmatrix} =$$

$$= \det(M_\gamma - x\,Id_5)^3$$

↑ apliquem prop determinat.

Per tant $P_c(x)$ és el cub del polinomi $\det(M_\gamma - x\,Id_5)$

(d) $\Rightarrow$ $\gamma \in M$.

γ és element primitiu $\Rightarrow M = \mathbb{Q}(\gamma)$

$\Rightarrow M = \mathbb{Q}\langle 1, \gamma, \gamma^2, \dots \gamma^{14} \rangle$

$\Rightarrow \boxed{\deg(\mathrm{Irr}(\gamma, \mathbb{Q}, x)) = 15}$

QUALIFICACIÓ

Assignatura: [redacted]

Estudiant/a:

Data:

$P_c(x)$

Sigui el polinomi característic associat a la representació matricial de φ en alguna base de M.

Pel teorema de Cayley-Hamilton.

$$P_c(\gamma) = 0 \Rightarrow \operatorname{Irr}(\gamma, \mathbb{Q}, x) \mid P_c(\gamma)$$

I sabem que $\deg(P_c(x)) = 15$.

$\deg(\operatorname{Irr}(\gamma, \mathbb{Q}, x)) = 15$.

$\Rightarrow P_c(\gamma) = \operatorname{Irr}(\gamma, \mathbb{Q}, x) \cdot c$ on $c \in \mathbb{K} - \{0\}$

$\Rightarrow P_c(\gamma)$ és irreductible. ✓

$\Leftarrow$ Fixem-nos que no ens calen condicions tan fortes. És suficient amb que el polinomi característic en una certa base sigui irreductible:

$\Rightarrow$ Ja demostrem que $\deg(\operatorname{Irr}(\gamma, \mathbb{Q}, x)) = 15$.

Suposem que és més petit que 15.

Sabem que en una certa base

$$P_c(\gamma) = 0 \quad \text{i} \quad P_c(\gamma) \text{ és irreductible}$$

pel teorema de Cayley-Hamilton i hipòtesis (injecció de M a matrius)

Llavors tenim que

$$Irr(\gamma, \mathbb{Q}, x) \mid P_c(\gamma)$$

$$\text{i} \quad gr(Irr(\gamma, \mathbb{Q}, x)) < gr(P_c(\gamma))$$

$\Rightarrow P_c(\gamma)$ no és irreductible $\Rightarrow \Leftarrow$

Per tant, $gr(Irr(\gamma, \mathbb{Q}, x)) = 15$.

$$\Rightarrow [\mathbb{Q}(\gamma) : \mathbb{Q}] = 15.$$

A més com $\gamma \in M$

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq M$$

i Com $[M : \mathbb{Q}] = 15$ per dimensió $\boxed{\mathbb{Q}(\gamma) = M}$ $\Rightarrow$ γ element primitiu.

Escaneado con CamScanner

4. A anell euclidià $\Rightarrow$ A anell principal.

Dem: Per definició, si A és un anell euclidià,

$\exists\ \delta: A\setminus\{0\} \longrightarrow \mathbb{N}$ tq.

(i) $\delta(a) \leq \delta(ab) \quad \forall a,b \in A\setminus\{0\}$

(ii) $\forall a,b \in A,\ b\neq 0 \quad \exists\ q,r \in A$ tq.

$a = bq + r$ i $\begin{cases} r = 0 \\ \text{o} \\ \delta(r) < \delta(b). \end{cases}$

Sigui I un ideal no nul. (sinó $I = (0)$ ✓)

Considerem el conjunt:

$$\delta(I) := \{\delta(a) : a \in I\setminus\{0\}\} \subseteq \mathbb{N}.$$

Pel principi de bona ordenació de $\mathbb{N}$.,

$$\exists\ m \left[\min \delta(I) = \delta(m)\right],\ m \in I.$$

Anem a demostrar que $I = (m)$

- En primer lloc, com $m \in I \Rightarrow (m) \subseteq I$ ✓
- En segon lloc, sigui $y \in I$ $(y \neq m, y \neq 0)$.

Com A és euclidià, sabem que $\exists\, q, r$ tq $y = mq + r$, on $\begin{cases} r = 0 \\ \delta(r) < \delta(m) \end{cases}$

↗ Si $r = 0 \Rightarrow y = mq \Rightarrow y \in (m)$ ✓

↘ Si $\delta(r) < \delta(m)$, tenim que

$$r = \underset{\in I}{y} - \underset{\in I}{mq} \in I \;;\; \delta(r) < \min \delta(I)$$

$\Rightarrow\Leftarrow$

Per tant, $\forall y \in I\ (y \neq m, y \neq 0)$, $y \in (m)$

$\Rightarrow I \subseteq (m)$ ✓

Finalment, tenim $I = (m)$ és principal.